AMENDMENTS TO THE CLAIMS:

Please replace the claims 1-13, as provided below. This listing of claims replaces all prior versions of the claims in the application.

Listing of Claims:

Claim 1. (Currently amended) A method for carrying out a secure digital signature of a person on a digital data packet(s) sent from a sender being a third party to ~~a~~ at least one recipient, said sender and said at least one recipient connected to a data network via network connection means, comprising the steps of:

a) sampling one or more biometric sample(s) of said person and converting said biometric sample(s) to a digital form;

b) storing said biometric sample at a location accessible to the sender;

c) storing, at the sender side, a digital packet(s) that may be altered by the at least one recipient at said sender side;

d) sending a request from the at least one recipient, to the sender, to select the digital data packet(s) to sign;

~~b)~~e) at said sender side, producing a first digital seal from the combination of said digital data packet(s) ~~wherein at least a portion of said data packet received from said recipient, and said biometric sample(s), or from two or more digital seals derived from said digital data packet(s) and said biometric sample(s)~~ and a one-time time stamp generated at said sender side using an asymmetric operator with the

private key of said sender and optionally with the public key of said at least one recipient;

~~e)~~f) sending said sealed digital data packet(s) ~~and said biometric sample(s) and said digital seal~~ to said at least one recipient;

~~d)~~g) ~~producing a second digital seal from said combinations of received digital data packet(s) and said received biometric sample(s)~~ at the at least one recipient side, receiving said sealed digital data packet(s) and opening said sealed digital data packet(s) with the sender's public key and optionally first with the at least one recipient's private key and then with the sender's public key;

h) allowing said at least one recipient to sign the opened digital data packet(s) by adding his biometric sample(s), in real-time, to said opened digital data packet(s);

i) at said at least one recipient side, producing a second digital seal from the combination of said signed digital data packet(s) and said one-time time stamp, using said asymmetric operator, with the public key of said sender and optionally with the private key of said at least one recipient;

j) at the sender side, receiving said sealed digital data packet(s) and opening said sealed digital data packet(s) with the sender's private key and optionally first with the at least one recipient's public key;

k) at the sender's side;

k.1) verifying that the signed digital data packet(s) has not been altered after sealing by the at least one recipient;

~~e)~~k.2) comparing ~~said first and said second seals~~ the biometric sample(s) attached to said opened digital data packet(s) with the at least one recipient's stored biometric sample(s); ~~and~~

~~f)~~k.3) if ~~said first and said second seals~~ the signed digital data packet(s) has not been altered after sealing by the at least one recipient and the biometric sample(s) attached to said opened digital data packet(s) and the at least one recipient's stored biometric sample(s) are identical, approving the authentication of said digital signature, otherwise denying the authentication of said digital signature; and

iv) providing the option of sending, by said sender, a receipt to all said recipients to confirm the authentication and receipt of said digital packet(s).

Claim 2. (Cancelled)

Claim 3. (Cancelled)

Claim 4. (Currently amended) A method according to claim 1 ~~or 2~~, ~~further~~ comprising the steps of:

a) providing a computerized server for managing the signing process, said server being connected to a network via network connection means;

b) providing a database system for storing signed data packet(s), unsigned data packet(s), a list of authorized users, said users' personal details and biometric templates, said database system accessible by said server;

c) providing one or more client terminal(s) for managing the signing process at the user's location, said terminal(s) being coupled with means for carrying out biometric samples, said terminals(s) being connected to said network via network connection means;

d) providing a list of users authorized for carrying out the digital signature, said users list, said users' personal details and their template(s) being stored in said database system;

e) providing a software component at the client's terminal for producing a template of a biometric sample;

f) providing another software component for comparing digital seals;

g) sending a request for carrying out the signature to said server;

At said server's location:

h) upon receiving a request for carrying out a digital signature from a client's terminal, generating a digital ID associated with said session;

i) sending said digital ID from said server to said client terminal;

At said client's location:

j) upon receiving a digital ID from said server, producing a digital package comprised of said digital ID, the personal information and the template and/or the image of a sample of said user;

k) adding a digital seal of said digital package to said digital package;

l) sending said digital package to said server;

m) identifying said user by the personal details comprised in said digital package;

n) authenticating said user's signature by comparing said received template with the template of said user which is stored in said database;

o) producing a second digital seal of said received digital package; and

p) upon positive results in said verification and said authentication and said comparison, approving the authentication of said digital signature, otherwise denying the authentication of said digital signature.

Claim 5. (Currently amended) A method according to ~~any one of~~ claims 1 ~~to 4~~or 2, further comprising the steps of:

a) providing means for encrypting and decrypting of data, said means residing on said server and said client(s);

b) encrypting any data to be sent; and

c) decrypting any received data.

Claim 6. (Currently amended) A method according to ~~claim 4~~ claim 2, wherein said digital ID is obtained randomly.

Claim 7. (Currently amended) A method according to ~~any one of~~ claims 1 ~~to 4~~or 2, wherein said digital seal is derived from a hash function.

Claim 8. (Currently amended) A method according to ~~any one of~~ claims 1 ~~to 4~~or 2, wherein said encryption-decryption is symmetric/asymmetric.

Claim 9. (Currently amended) A method according to ~~any one of~~ claims 1 ~~to 4~~or 2, wherein said biometric sample(s) is chosen from fingerprint(s), voice, speech, face, retina, iris, handwritten signature, hand geometry, veins.

Claim 10. (Currently amended) A method according to ~~any one of~~ claims 1 ~~to~~ 4or 2, wherein said data is sent via the Internet and/or via the Intranet and/or via a WAN (Wide Area Network) and/or via a LAN (Local Area Network) and/or via a WAP (Wireless Application Protocol) and/or via the telephone network and/or by FTP (File Transfer Protocol) and/or by e-mail.

Claim 11. (Currently amended) A system for carrying out secure ~~digital signature on one or more~~ signing of a person on a digital data packet(s) sent from a sender being a third party to at least one recipient, said sender and said at least one recipient connected to a data network via network connection means, comprising:

- a computerized server for managing the signing process, said server being connected to ~~a~~ said data network via said network connection means;

- a database system for storing signed data packets, unsigned data packets, a list of authorized users, said users' personal details and biometric templates, said database system accessible by said server;
- ~~one or more client~~ a sender's terminal~~(s)~~ for managing the signing process at the ~~user's location for the signing of data packets which are received from said server~~ sender's side, ~~said terminal(s) being coupled with means for carrying out biometric samples, and~~ connected to said network via network connection means;
- one or more recipient's terminals for performing the signing process at the recipient side, said one or more recipient's terminals being coupled with means for carrying out a biometric sample(s) of said at least one recipient, and connected to said network via network connection means;
- a software component at said sender's terminal, which after receiving a request from said at least one recipient to select the digital data packet(s) to sign, produces a first digital seal from the combination of said digital data packet(s), and produces a one-time time stamp using an asymmetric operator, and then sends said sealed digital data packet(s) to said one or more recipient's terminals;
- a second software component at ~~the client's terminal for producing a template of a biometric sample~~ said one or more recipient's terminals for receiving said sealed digital data packet(s), for opening said sealed digital data packet(s), for allowing said at least one recipient to sign

the opened digital data packet(s) by adding his biometric sample(s) to said opened digital data packet(s), for producing a second digital seal from the combination of said signed digital data packet(s) and said one-time time stamp, using said asymmetric operator; and

- a third software component for ~~comparing digital seals~~ verifying that the signed digital data packet(s) has not been altered after sealing by said at least one recipient and comparing the biometric sample(s) attached to said opened digital data packet(s) with the at least one recipient's stored biometric sample(s).

Claim 12. (Currently amended) A system according to claim 11, further comprising means for encrypting and decrypting of data, said means residing on said server, and said ~~client(s)~~ sender's terminal~~(s)~~, and said one or more recipient's terminals.

Claim 13. (Currently amended) A system according to claim 11, wherein said ~~client's~~ sender's terminal is a computer or a set-top box or a mobile phone and said one or more recipient's terminals are any combination of computers, or set-top boxes, or mobile phones.